A I

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80546 A2

(51) International Patent Classification[7]: H04N

(21) International Application Number: PCT/IL01/00295

(22) International Filing Date: 29 March 2001 (29.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/549,820 14 April 2000 (14.04.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/370,813 (CIP)
Filed on 9 August 1999 (09.08.1999)

(71) Applicant *(for all designated States except US)*: **MIDBAR TECH LTD.** [IL/IL]; 34 Kibbutz Galuyot Street, 66550 Tel Aviv (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ALCALAY, Ran** [IL/IL]; 24 Nachum Street, 63503 Tel Aviv (IL). **SINQUIN, Patrice** [FR/IL]; 14 Bar Kochva Street, 63426 Tel Aviv (IL). **SELVE, Philippe** [IL/IL]; 13 Yossef Hanasi Street, 65236 Tel Aviv (IL).

(74) Agents: **COLB, Sanford, T.** et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

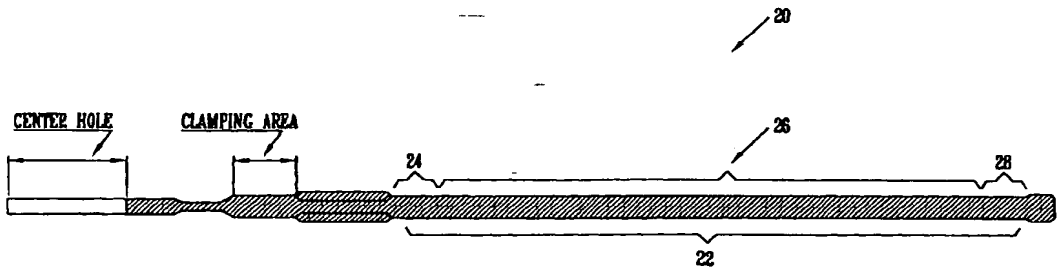
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PREVENTION OF CD-AUDIO PIRACY USING SUB-CODE CHANNELS



(57) Abstract: A method for protecting data recorded on an original storage medium (20) against copying using an unauthorized data readout device. The data are encoded in accordance with Standard 908 of the International Electrotechnical Commission. A portion of the encoded data is altered to introduce a modification in a sub-code Q channel of the data, such that the altered data are inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof. The data, including the altered data, are recorded on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

WO 01/80546 A2

PREVENTION OF CD-AUDIO PIRACY USING SUB-CODE CHANNELS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of co-pending U.S. Patent Application 09/549,820, filed April 14, 2000, which is a continuation-in-part of U.S. Patent Application 09/370,813, filed August 9, 1999, which is a continuation-in-part of U.S. Patent Application 09/175,255, filed October 20, 1998. All of these applications are assigned to the assignee of the present patent application and are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to protection of intellectual property rights, and specifically to prevention of unauthorized copying of recorded audio, computer-readable media.

BACKGROUND OF THE INVENTION

Compact disk (CD) recordings are a preferred means for distributing both digital audio recordings and computer software. CD audio recordings are almost universally made in accordance with standard 908 of the International Electrotechnical Commission (IEC), entitled "Compact Disc Digital Audio System" (Geneva, Switzerland, 1987), which is incorporated herein by reference. The 908 standard, also known as the Red Book, defines how audio data are to be encoded and recorded on the disk, enabling the data to be played back using standard digital decoding chips. Different standards apply to other types of data, such as computer software, which may be recorded on CD, as well. For example, the Blue Book standard specifies multi-session recordings, that combine audio and other data on a single disk.

Original music CDs are produced by molding plastic blanks with a master stamp piece, which is produced using costly, specialized equipment. Alternatively, a recordable CD (CDR) may be created by authorized plants according to customer request. Because of the high cost of CD recording equipment, CD recordings were considered, until recently, to be relatively secure against unauthorized copying. This situation has changed recently, as inexpensive CD recording devices and read/write media have become available to consumers. Thus, it is now easy, using a conventional personal computer with a read/write CD drive, or with one read drive and one write drive, to make exact, digital copies of all types of CDs. The CD content is

read out by the computer, byte by byte, from one CD, typically a legitimately-purchased original CD, and then written to a blank CD so as to make a pirate copy. Similar copying methods may be used with other media, such as Digital Video Disks (DVD). Financial losses to the recording and software industries due to such pirate copying are estimated to be in the billions of dollars.

Another common method for pirate copying is via the digital audio output provided by many CD players, such as the S/PDIF (Sony/Philips Digital Interconnect Format) output. This output format is specified by IEC standard 958, entitled "Digital Audio Interface" (Geneva, Switzerland, 1993), which is incorporated herein by reference. The S/PDIF output can be used legitimately to connect the CD player to high-quality converters, speakers and other audio components. On the other hand, since it reproduces the audio content of the CD bit by bit, the S/PDIF output is also easy for pirates to use in making illegal copies. In addition to the audio content, the S/PDIF data includes a sub-code, known as the serial copying management system (SCMS) sub-code, that indicates whether the source of the data is an original recording or a copy. According to SCMS, commercially-available recording equipment is not supposed to allow users to record audio from a S/PDIF stream that is marked as a copy. This protection, however, is easily circumvented by pirate copiers.

SUMMARY OF THE INVENTION

It is an object of some aspects of the present invention to provide improved methods and apparatus for preventing unauthorized copying of recorded, computer-readable media.

It is a further object of some aspects of the present invention to provide methods and apparatus for producing compact disks that are resistant to unauthorized copying.

It is still a further object of some aspects of the present invention to provide methods and apparatus for preventing unauthorized digital copying of audio disks.

In preferred embodiments of the present invention, signals recorded on an original storage medium are protected against unauthorized copying by changes made in a sub-code channel, preferably the Q-channel. For this purpose, a data-writing unit comprises an encoding block, which receives audio signals and encodes the signals in accordance with standard 908 of the International Electrotechnical Commission (IEC). A modification-insertion block of the data-writing unit alters the encoded signals, by introducing a modification in a sub-code Q

channel of the encoded signals. A recording block of the data-writing unit subsequently records the altered signals on the storage medium, which typically comprises a compact disk (CD).

Preferably, the altered signals are erroneous according to standard 908, or according to implementations of the standard used in CD-ROM drives, but nevertheless do not prevent playback of the audio signals from the original medium following recording. Thus, the original CD is able to perform in a manner substantially unaffected by the alteration. By contrast, the alteration causes a substantially-unrecoverable error when an attempt is made to create an unauthorized copy of the CD. The error manifests itself in that either the unauthorized copy cannot be produced at all, or the copy is corrupted in such a way as to render it substantially unusable. Preferably, authorized software residing in the data-writing unit or in other hardware is enabled to duplicate the CD, such that authorized copies also can be played back, unaffected by the alteration.

In some preferred embodiments of the present invention, the modification-insertion block inserts the modification in the sub-code Q channel by specifying a modified absolute or relative track time of the audio signals recorded on the CD. CD copying algorithms known in the art rely on non-corrupted track times, and are therefore unable to make unauthorized copies of CDs which are prepared using these embodiments of the present invention. Optionally, the original track time is stored on the original CD in reserved bits of the sub-code channels that are defined by standard 908. Authorized copying software retrieves the original track time from the reserved bits, and is thereby enabled to make fully-functioning copies of the original CD.

Alternatively or additionally, the modification is introduced by adding one or more additional sessions on the disk, with a lead-in that point to tracks in the program area of the first session and includes special modes to block an unauthorized computer from reading the session.

Further alternatively or additionally, the modification-insertion block inserts the modification in the sub-code Q channel by specifying a modified index number of a track of the audio signals recorded on the CD. CD copying algorithms known in the art rely on the non-corrupted index number of the track, and are therefore unable to make unauthorized

copies of CDs which are prepared using these embodiments of the present invention. Optionally, the original index number of a track is stored on the original CD in reserved bits of the sub-code channels that are defined by standard 908. Authorized copying software retrieves the original index number of the track from the reserved bits or from a second session on the disk, and is thereby enabled to make fully-functioning copies of the original CD.

Preferably, in order to allow an authorized personal computer (PC) to play the contents of the protected disk, the original contents are protected by digital rights management (DRM) technology, typically by compressing (using any suitable format known in the art, such as MP3 or VQF) and encrypting the contents. These encrypted data are stored in a manner that is hidden to conventional CD driver software, for example in reserved sub-code channel bits, in the pause area or lead-out area, or in a second session on the CD. The data can be decrypted and played back only by using authorized software, which is preferably stored in the second session.

Further preferably, the modifications introduced in the CD are such as to cause changes in a S/PDIF output or other digital output generated by a CD player in which the protected CD is played. The changes in the digital output do not interfere with audio playback of the CD recording by compatible equipment, such as audio speakers with a digital/analog converter. The changes do, however, prevent unauthorized copying of the CD content using the digital output, for example, as a digital input to a recorder.

Optionally, in addition to the modifications introduced in the sub-code channel, further modifications are intentionally introduced in the audio data as an added impediment to unauthorized copying. The modifications are introduced in such a way that ancillary data on the disk, such as error detection codes, which are provided by the 908 standard (or other applicable standard), enable a CD player either to correct or conceal the modifications during playback or to ignore them altogether. When an unauthorized copy is made of the medium, however, the ancillary data are ineffective in overcoming the intentional modifications in the original medium, with the result that faults occur in the copy that are substantially unrecoverable. Methods for introducing such modifications are described in the above-mentioned U.S. Patent Applications 09/175,255 and 09/370,813.

There is therefore provided, in accordance with a preferred embodiment of the present

invention, a method for protecting data recorded on an original storage medium against copying using an unauthorized data readout device, the method, including:

receiving data encoded in accordance with Standard 908 of the International Electrotechnical Commission;

altering a portion of the encoded data to introduce a modification in a sub-code Q channel of the data, such that the altered data are inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof; and

recording the data, including the altered data, on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

Preferably, the medium includes a compact disk, and the data include digital audio data.

In a preferred embodiment, altering the data includes modifying an absolute time in the data to be recorded on the medium. Preferably, a correct absolute time is stored in reserved sub-code bits on the medium. Most preferably, modifying the absolute time includes altering absolute times recorded in a plurality of consecutive blocks of a selected track.

In another preferred embodiment, altering the data includes duplicating one or more blocks of the data to a new location on the storage medium, without changing the absolute time recorded in the sub-code Q channel of the one or more blocks.

In still another preferred embodiment, altering the data includes modifying a point index number in a track of the data to be recorded on the medium. Preferably, the method includes storing a correct index number in reserved sub-code bits on the medium.

In yet another preferred embodiment, altering the data includes generating a multiple-session recording, including one or more audio and data sessions, wherein the modification in the sub-code Q channel is introduced in one or more of the data and audio sessions. Preferably, generating the multiple-session recording includes creating a lead-in to one of the sessions that points to one or more tracks located in a first audio session on the

medium. Alternatively or additionally, generating the multiple-session recording includes creating a lead-in to one of the sessions that includes a larger number of tracks than is specified by the standard. Further alternatively or additionally, generating the multiple-session recording includes creating a lead-in to one of the sessions that indicates that the recording medium is shorter than it is in actuality. Still further alternatively or additionally, generating the multiple-session recording includes inserting a modified absolute time at a start of one of the sessions. Yet further alternatively or additionally, generating the multiple-session recording includes creating multiple sessions at least two of which are identified as audio sessions.

In a preferred embodiment, recording the data includes compressing and storing the data in a data session on the medium, for use in making an authorized copy of the medium.

In a further preferred embodiment, the encoded data include encoded audio data, and the method includes altering a portion of the encoded audio data such that the altered data are inconsistent with the implementation of Standard 908 used in the data readout device, wherein recording the data on the medium includes recording ancillary data which are used by a processor in the application to operate upon the altered portion of the encoded audio data such that the application plays back the data in a manner substantially unaffected by the alteration of the encoded audio data, but which ancillary data are ineffective in correcting the altered portion of the encoded audio data upon copying of the data, so that the alteration causes a further substantially unrecoverable error in the unauthorized copying of the original medium.

Preferably, the ancillary data include error detection codes.

There is further provided, in accordance with a preferred embodiment of the present invention, a method for protecting data recorded on an original storage medium against unauthorized copying, including:

receiving data encoded in accordance with Standard 908 of the International Electrotechnical Commission;

altering a portion of the encoded data to introduce a modification in the data, so that a digital output of the altered data will be inconsistent with an implementation of a digital output standard, such as Standard 958 of the International Electrotechnical Commission, but the modification will not prevent playback of the data following recording thereof; and

recording the data, including the altered data, on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the modification in the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium based on the digital output.

Preferably, altering the portion of the encoded data includes altering one or more control bits in the encoded data, which control bits are reproduced in the digital output. Additionally or alternatively, altering the portion of the encoded data includes manipulating bits of audio data within a frame of the encoded data.

There is also provided, in accordance with a preferred embodiment of the present invention, apparatus for protecting data recorded on an original data storage medium against copying using an unauthorized data readout device, including:

an encoder, adapted to receive a stream of data for recording on the medium and encodes the data in accordance with Standard 908 of the International Electrotechnical Commission;

a sub-code generator, operative to alter a portion of the encoded data by introducing a modification in a sub-code Q channel of the data, such that the altered data are inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof; and

an eight-to-fourteen bit (EFM) modulator, coupled to modulate the altered data for recording on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

In a preferred embodiment, the apparatus includes a data session generator, operative to provide a data session to the EFM for recording on the original storage medium, so that the data recorded on the medium include multiple-session data, and the defect in the sub-code Q channel is introduced in at least one of the multiple sessions.

There is additionally provided, in accordance with a preferred embodiment of the present invention, a data storage medium that is resistant to copying using an unauthorized

readout device, on which medium data encoded in accordance with Standard 908 of the International Electrotechnical Commission are stored, a portion of which encoded data is altered by introducing a modification in a sub-code Q channel of the data, such that the altered data are identified as inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

The present invention will be more fully understood from the following detailed description of the preferred embodiments thereof, taken together with the drawings in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic, sectional view of a compact disk (CD), in accordance with recording practice known in the art;

Fig. 2 is a schematic block diagram that illustrates apparatus for producing a copy-resistant CD, in accordance with a preferred embodiment of the present invention;

Fig. 3 is a schematic illustration of details of a data structure written to a CD, in accordance with recording practice known in the art; and

Fig. 4 is a block diagram that schematically illustrates duplication of data on a CD for the purpose of preventing unauthorized copying, in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1, which is a schematic sectional view of an audio compact disk (CD) 20, showing the overall layout of the disk, in accordance with recording practice known in the art. An information area 22 includes a lead-in (LI) area 24, a program area (PA) 26 and a lead-out (LO) area 28. Information area 22 progresses outwards in a widening spiral, and contains all of the recorded contents of CD 20. Lead-in area 24 and lead-out area 28 both contain P and Q channels, which include timing and track information used during playback of the CD. Program area 26 consists of up to 99 tracks of audio information (e.g., music), as well as accompanying sub-code information.

Preferred embodiments of the present invention provide a number of different, complementary techniques for modifying the data in CD 20 in order to frustrate pirate copiers. A number of these embodiments are described in detail hereinbelow. Generally speaking, the modifications fall into the following categories:

- General disk layout modifications – for example, recording several sessions on an audio CD. The second session can be used to mislead personal computers (PCs) that are commonly used in pirate copying, typically by adding conflicting pointers in the lead-in of the second session. Preferably, the last session on the CD is a data session that contains the music in compressed form. Most preferably, the music is encrypted so as to enable playback directly from the disk and/or encoded using digital wrapper technology (also known as digital rights management – DRM) to enable download and playback through secure software from the disk of an authorized user.

- Modifications of the audio data, by insertion of noise, preferably as described in the above-mentioned U.S. Patent Application 09/370,813.

- Modifications of the subcode information, particularly in the Q channel. These modifications may include, for example, changing the absolute or relative time, index pointers, table of contents (TOC) information (listing too many or too few tracks, or misleading pointers between multiple sessions), control byte modifications, pregap length manipulation. Other such modifications will be apparent to those skilled in the art.

- Low-level modifications to the structure of the bits recorded on the CD. Such modifications are described in detail in the above-mentioned U.S. Patent Applications 09/175,255 and 09/370,813. They typically involve recording sequences of bits on the CD that cause hardware errors in some CD-ROM drives used in PCs, or prevent them from interpolating over erroneous audio data. Alternatively or additionally, bit sequences may be recorded on the CD that do not appear in the conventional eight-to-fourteen bit (EFM) lookup table specified by the 908 standard.

These modifications may be used in CD 20 in different combinations, depending on application needs.

Fig. 2 is a schematic block diagram that illustrates apparatus 40 for producing a copy-resistant CD, in accordance with a preferred embodiment of the present invention. The original sound, or analog audio, is converted to digital format suitable for encoding on a disk, such that the information can subsequently be played back (decoded) by a standard player of audio CD 20. In a first stage of encoding, a digital bit stream is generated which represents the continuous analog sound signal. The analog signal is converted into discrete digital samples by an analog-to-digital (A/D) converter 30.

To enable detection and correction of errors during playback, parity bits are added to the bit stream. An error-correction encoder 32 employs the commonly used Cross-Interleaved Reed-Solomon Code (CIRC) to reorder the digital data. A sub-code generator 36 adds a byte of sub-code for every thirty-two bytes of error-corrected audio. The 908 standard prescribes the contents of the sub-code channels to be added at this stage. Sub-code generator 36, however, alters the standard sub-codes in such a manner that ordinary playback of the CD is substantially unaffected, but unauthorized copying is prevented. In particular, the alterations do not compromise the integrity of the bit stream and do not generate CIRC errors on the disk. Methods of such alteration are described hereinbelow.

Apparatus 40 is also shown to include an optional data session generator 37, for use in producing multiple-session disks that include both audio and data sessions. As described hereinbelow, the data session is configured so as to prevent an unauthorized computer from reading the CD. An audio compressor 35 is optionally provided to compress the audio input for inclusion in such a multiple-session disk in an encoded form.

It is known in the art to map a standard sixteen-bit word of sound data into two fourteen-bit "optical" symbols, and to include in the recording additional information, such as playback control and display functions. An eight-to-fourteen modulator (EFM) 34 combines the output of error-correction encoder 32 with the output of sub-code generator 36 and data session generator 37. Each bit of encoded data is preferably physically inscribed onto a master for producing CD 20, using a laser beam recorder (LBR) 38 to create a series of microscopic pits on the master. Alternatively, a dedicated burner 39 is used to produce CD 20 directly on a recordable CD (CDR).

Fig. 3 is a schematic illustration of details of the data structure received by EFM modulator 34, in accordance with the 908 standard. A block 58 of data for recording on a CD contains 98 frames, each frame made up of 32 bytes of data, or symbols, received from encoder 32 (or from the data session generator 37) and one eight-bit "sub-code" word. The eight bits in each sub-code word are respectively called P, Q, R, S, T, U, V, and W.

The Q bits from 98 consecutive frames are collectively called a sub-code Q channel 64. The sub-code Q channel contains program and timing information, including synchronization bits S0 and S1, 4 control bits, 4 address bits, 72 data bits, and a 16-bit cyclic redundancy check code (CRCC). In lead-in area 24, the 72 data bits include relative time (R-Time, or track time) data 74 and track position, while in program area 26, relative time and absolute time (A-Time, or disk time) data are stored. The relative time for each block indicates the length of time from the beginning of a current track to the beginning of the block. The absolute time indicates the length of time from the beginning of program area 26 to the beginning of the block. Time is measured in units of minutes, seconds and frames (different from the 98 data frames in a block), with 75 time frames in a second. The Q channel also includes a track number (TNO) and in-track indices, also referred to as point indices. In lead-in area 24, the Q channel carries a table of contents (TOC).

Table I below schematically illustrates alteration of absolute time values of sub-code Q channel 64, in accordance with a preferred embodiment of the present invention. In typical encoding of CD 20 according to standard 908, absolute time starts at the beginning of program area 26 and increases linearly to the end of lead-out area 28. Copying software known in the art uses the absolute time as a pointer, in order to ensure smooth reproduction of the original audio and synchronicity of timing between recorded frames and played-back frames. Preferably embodied, a modification is introduced into the absolute time values of the sub-code Q channel, as shown in the "altered" column in the table, thereby increasing the speed at which time appears to pass in this track.

TABLE I

Original time			Altered time		
Min	Sec	Frame	Min	Sec	Frame
0 (start	0	0	0	0	0

track)					
0	0	1	0	0	2
0	0	2	0	0	4
0	0	3	0	0	6
0	0	4	0	0	7
0	0	5	0	0	8
...	...	...	...	...	...
0	0	71	0	0	74
0	0	72	0	1	0
...	...	...	...	...	...
5 (end track)	30	42	5	36	20
5 (pause)	30	43	5	30	43
5	30	44	5	30	44
...	...	...	...	...	...

So as not to adversely affect stereo play-back of the audio, the absolute time for original CD 20 is preferably increased in several consecutive blocks out of every 150 consecutive blocks, and returned to normal in a pause area between tracks, as shown in the table above. A standard CD player will be unaffected by these intentional distortions of the absolute time. An unauthorized copy of CD 20, however, will contain discontinuities in the music, for example, where absolute time jumps from frame 2 to frame 4 to frame 6, in the table above. The resulting signal on the CD copy will have a series of constant-amplitude, audible, distorted and generally unmelodious sounds.

Optionally, the original, correct absolute time information is stored in the reserved bits of the sub-code R-W channels (Fig. 3), which are currently unassigned according to standard 908. Authorized software is enabled to make copies of original CD 20 by accessing the data stored in the R-W channels.

Alternatively, rather than introducing modifications in the absolute time, modifications that produce audible effects in unauthorized copies are introduced in sub-code Q channel 64 by

changing point index and/or mode values. Like the absolute track time, the point index provides a series of "checkpoints" within a track. A modified series of point indices will cause mute areas in an unauthorized copy of CD 20, but will not affect the playback of the original CD. Optionally, as described above, the correct indices are stored in the R-W channels, and authorized software is enabled to copy the original CD by retrieving the indices from these channels.

Preferably, modifications introduced in the CD are such as to cause changes in a digital output, such as a S/PDIF output, generated by a CD player in which the protected CD is played. The digital output data stream comprises a sequence of 32-bit words, known as sub-frames, each carrying between 16 and 24 bits of audio data, along with preamble and control bits. One of the control bits in each sub-frame is a sub-code bit, similar to the sub-code bits in each frame of data on the CD. The sub-code bits in a block of 192 frames (typically 384 sub-frames) in the S/PDIF data stream carry most of the contents of the sub-code Q channel being played on the CD, including control bytes, the track number and the time. Preferably, the modifications that are introduced in the Q channel on the disk are such as to be carried over to the S/PDIF data. Although these modifications do not interfere with audio playback of the CD recording by speakers and other compatible equipment, they do impede unauthorized copying of the CD content using the digital output.

As specified by the above-mentioned IEC 958 standard, the S/PDIF signal contains four control bytes copied from the CD. Therefore, in an alternative embodiment of the present invention, these control bytes are used to frustrate illegal copying of the audio contents. For this purpose, in recording the control bytes on the CD, in accordance with the Red Book standard, the track mode is set to "data" for a number of blocks, typically between one and ten blocks, in a repetitive cycle. The CRCC is then recalculated so that this control byte is valid from the standpoint of data accuracy. When a recording is made from the S/PDIF output of the CD player, however, this control byte setting will typically cause mutes or clicks to appear in the resulting audio stream.

In a further alternative embodiment, the bits in the S/PDIF envelope are shifted or otherwise manipulated in order to confound unauthorized recording of the CD contents. When the 32 bits in a S/PDIF sub-frame are fed to a digital/analog converter for audio playback, the converter takes all 32 bits and plays back the audio irrespective of the shift. A digital recorder,

however, will seek the audio data in a given subset of the bits of the sub-frame, and the control data in another subset, disjoint from the audio data, where these data are supposed to be according to the standard. Therefore, manipulating the bit order can block recorders while still enabling audio playback.

Fig. 4 is a block diagram that schematically illustrates another method for preventing unauthorized copying of a CD, using data session generator 37, in accordance with a preferred embodiment of the present invention. Whereas an audio CD has only a single session 90, apparatus 40 with session generator 37 can produce CDs having multiple sessions, including, for example, one or more audio sessions 100 and at least one data session 102. Audio CD players read only the first session on a multiple-session CD, in this case session 100 and ignore the rest. DVD players read and are "aware" of data session 102, as well, but still play back audio session 100. When the CD is inserted into a CD-ROM drive, however, the computer can access any of the sessions and therefore will be confused by the modifications embedded in the second or subsequent sessions. The present embodiment therefore operates by introducing conflicting data into the sub-code Q channel of data session 102 or of additional audio sessions, subsequent to the first audio session. Most preferably, there are at least two audio sessions out of a total of three or more sessions on the disk.

Preferably, modified data are introduced into audio session 100, as well. The modifications are introduced in such a way that ancillary data on the disk, such as Cross Interleave Reed Solomon Code (CIRC) error detection codes, which are provided by the 908 standard (or other applicable standard), enable a CD player either to correct or conceal the modifications during playback or to ignore them altogether. When an unauthorized copy is made of the medium, however, the ancillary data are ineffective in overcoming the intentional modifications in the original medium, with the result that faults occur in the copy that are substantially unrecoverable. Methods for introducing such modifications are described in the above-mentioned U.S. Patent Applications 09/175,255 and 09/370,813.

Despite the modifications in the sub-code channels and/or audio data, an audio CD player will reproduce the audio signals on the disk without difficulty. A computer CD drive, however, will be confused by either the multiple sessions on the CD or the modified data in audio session 100 (or by both) and will not be able to load or play the disk, let alone copy it.

Modifications in the added audio and/or data sessions are preferably introduced by one or more of the following mechanisms:

- Generating a lead-in that points to tracks located in the program area of the first session.
- Generating a lead-in with a larger number of tracks than is allowed by the 908 standard.
- Modifying the lead-in to simulate a shorter CD.
- Modifying the absolute time at the beginning of the session.

Following these methods, Table II below describes changes made in the sub-code Q channel of a multiple-session CD, in order to prevent computer copying of the audio content without interfering with audio playback. The first session on the CD is an audio session, based on the Red Book standard, while the second and subsequent sessions may be audio or data sessions, based on the Blue Book, as described above.

TABLE II

Session	Standard	Modification
1	Lead-in (2½-3 min)	Add pointers B0 and C0 to the second and third sessions, per Blue Book format.
	Pause length 2 sec	Use different pregap length, per Blue Book format, preferably set to value between 1 and 3 sec.
	Accurate A-Time	Start A-Time at non-zero value, e.g., 10 sec, to mask beginning of disk for computer CD drive.
2	Audio track	Audio track length 4 sec (minimum time per Red Book).
3	Lead-in (1 min)	TOC points to 99 non-existent data tracks at time 00:02. Modify lead-out pointer (A2) to a value between 00:01 and 00:07.

	Audio track	Data track length 4 sec, plus fill to a total CD length.

As a result of these changes, a computer CD-ROM or DVD-ROM drive, upon reading the sub-code Q channel data in session 3, will either fail to mount the CD entirely, or will go into an endless loop looking for the non-existent data tracks listed in the TOC. If the drive does succeed in accessing session 1, which holds the normal audio content, it is still likely to be confused by the 1 sec pregap (which is outside the Red Book specification) and/or by the distorted A-time. CD audio and DVD players, however, will be largely unaffected by these changes. In this regard, session 2 is important, since without it, some Blue Book-compliant DVD players might refuse to mount the CD. It will be understood that the specific modifications noted in the table are listed by way of example. Alternative combinations of modifications and settings of the time values and other parameters will be apparent to those skilled in the art.

Preferably, in order to allow an authorized personal computer (PC) to play the contents of the protected disk, the original contents are compressed (using any suitable format known in the art, such as MP3 or VQF) and encrypted, by audio compressor 35 (Fig. 2). These encrypted data are stored using a "digital wrapper" technique, so that the data are hidden from conventional CD driver software. For example, the data may be stored in the reserved sub-code channel bits, as described above, or in one of the data sessions on the CD, or in a lead-in, lead-out or pause area. The data can be decrypted and played back only by using authorized software, which is also preferably stored in the second session and is made available only to appropriately-licensed users and/or equipment. The authorized software will prevent the decryption of the data if its source is not the original CD or if the rules for distributing and using the data are otherwise violated.

It will be appreciated that the preferred embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art.

CLAIMS

1. A method for protecting data recorded on an original storage medium against copying using an unauthorized data readout device, the method comprising:

receiving data encoded in accordance with Standard 908 of the International Electrotechnical Commission;

altering a portion of the encoded data to introduce a modification in a sub-code Q channel of the data, such that the altered data are inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof; and

recording the data, including the altered data, on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

2. A method according to claim 1, wherein the medium comprises a compact disk.

3. A method according to claim 1, wherein the data comprise digital audio data.

4. A method according to claim 1, wherein altering the data comprises modifying an absolute time in the data to be recorded on the medium.

5. A method according to claim 4, and comprising storing a correct absolute time in reserved sub-code bits on the medium.

6. A method according to claim 4, wherein modifying the absolute time comprises altering absolute times recorded in a plurality of consecutive blocks of a selected track.

7. A method according to claim 1, wherein altering the data comprises duplicating one or more blocks of the data to a new location on the storage medium, without changing the absolute time recorded in the sub-code Q channel of the one or more blocks.

8. A method according to claim 1, wherein altering the data comprises modifying a point index number in a track of the data to be recorded on the medium.

9. A method according to claim 8, and comprising storing a correct index number in reserved sub-code bits on the medium.

10. A method according to claim 1, wherein altering the data comprises generating a multiple-session recording, including audio and data sessions, wherein the modification in the sub-code Q channel is introduced in at least one of the sessions.

11. A method according to claim 10, wherein the sessions comprise a first audio session, and wherein generating the multiple-session recording comprises creating a lead-in to one of the sessions that points to one or more tracks located in the first audio session.

12. A method according to claim 10, wherein generating the multiple-session recording comprises creating a lead-in to one of the sessions that includes a larger number of tracks than is specified by the standard.

13. A method according to claim 10, wherein the modification is introduced in both the audio and data sessions.

14. A method according to claim 10, wherein generating the multiple-session recording comprises inserting a modified absolute time at a start of one of the sessions.

15. A method according to claim 10, wherein generating the multiple-session recording comprises creating multiple sessions at least two of which are identified as audio sessions.

16. A method according to claim 1, wherein recording the data comprises compressing and storing the data in a data session on the medium, for use in making an authorized copy of the medium.

17. A method according to claim 1, wherein the encoded data comprise encoded audio data, and comprising altering a portion of the encoded audio data such that the altered data are identified as inconsistent with the implementation of Standard 908 used in the data readout device,

wherein recording the data on the medium comprises recording ancillary data which are used by a processor in the application to operate upon the altered portion of the encoded audio data such that the application plays back the data in a manner substantially unaffected by the alteration of the encoded audio data, but which ancillary data are ineffective in correcting the altered portion of the encoded audio data upon copying of the data, so that the alteration causes a further substantially unrecoverable error in the unauthorized copying of the original medium.

18. A method according to claim 17, wherein the ancillary data comprise error detection codes.

19. A method according to claim 1, wherein altering the portion of the encoded data comprises altering the data so as to create the modification in a standard digital output generated from the medium.

20. A method according to claim 19, wherein the standard digital output is generated in accordance with Standard 958 of the International Electrotechnical Commission.

21. A method for protecting data recorded on an original storage medium against unauthorized copying, comprising:

receiving data encoded in accordance with Standard 908 of the International Electrotechnical Commission;

altering a portion of the encoded data to introduce a modification in the data, so that a digital output of the altered data will be inconsistent with an implementation of Standard 958 of the International Electrotechnical Commission, but the modification will not prevent playback of the data following recording thereof; and

recording the data, including the altered data, on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the modification in the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium based on the digital output.

22. A method according to claim 21, wherein altering the portion of the encoded data comprises altering one or more control bits in the encoded data, which control bits are reproduced in the digital output.

23. A method according to claim 21, wherein altering the portion of the encoded data comprises manipulating bits of audio data within a frame of the encoded data.

24. Apparatus for protecting data recorded on an original data storage medium against copying using an unauthorized data readout device, the apparatus comprising:

an encoder, adapted to receive a stream of data for recording on the medium and to encode the data in accordance with Standard 908 of the International Electrotechnical Commission;

a sub-code generator, operative to alter a portion of the encoded data by introducing a modification in a sub-code Q channel of the data, such that the altered data are inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof; and

an eight-to-fourteen bit (EFM) modulator, coupled to modulate the altered data for recording on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

25. Apparatus according to claim 24, wherein the medium comprises a compact disk.

26. Apparatus according to claim 24, wherein the data comprise digital audio data.

27. Apparatus according to claim 24, wherein the modification in the sub-code Q channel comprises an altered value of the absolute time of a track of the data to be recorded on the medium.

28. Apparatus according to claim 24, wherein the modification in the sub-code Q channel is engendered by duplicating one or more blocks of the data to a new location on the storage medium, without changing the absolute time recorded in the Q channel of the one or more blocks.

29. Apparatus according to claim 24, wherein the modification in the sub-code Q channel comprises a modified value of the point index number of a track of the data to be recorded on the medium.

30. Apparatus according to claim 24, and comprising a data session generator, operative to provide a data session to the EFM for recording on the original storage medium, so that the data recorded on the medium comprise multiple sessions, and the defect in the sub-code Q channel is introduced in at least one of the multiple sessions.

31. Apparatus according to claim 24, wherein the encoded data comprise encoded audio data, and the encoder is further operative to alter a portion of the encoded audio data such that the altered data are identified as inconsistent with the implementation of Standard 908 used in the data readout device,

wherein the data recorded on the medium comprise ancillary data which are used by a processor in the application to operate upon the altered portion of the encoded audio data such that the application plays back the data in a manner substantially unaffected by the alteration of the encoded audio data, but which ancillary data are ineffective in correcting the altered portion of the encoded audio data upon copying of the data, so that the alteration causes a further substantially unrecoverable error in the unauthorized copying of the original medium.

32. Apparatus according to claim 24, wherein the defect in the sub-code Q channel is such as to create the modification in a digital output generated from the medium in accordance with Standard 958 of the International Electrotechnical Commission.

33. Apparatus for protecting data recorded on an original storage medium against unauthorized copying, comprising:

an encoder, adapted to receive a stream of data for recording on the medium and to encode the data in accordance with Standard 908 of the International Electrotechnical Commission, while altering a portion of the encoded data to introduce a modification in the data, so that a digital output of the altered data will be inconsistent with an implementation of Standard 958 of the International Electrotechnical Commission, but the modification will not prevent playback of the data following recording thereof; and

an eight-to-fourteen bit (EFM) modulator, coupled to modulate the altered data for recording on the original storage medium, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the modification in the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium based on the digital output.

34. Apparatus according to claim 33, wherein altering the portion of the encoded data comprises altering one or more control bits in the encoded data, which control bits are reproduced in the digital output.

35. Apparatus according to claim 33, wherein altering the portion of the encoded data comprises manipulating bits of audio data within a frame of the encoded data.

36. A data storage medium that is resistant to copying using an unauthorized readout device, on which medium data encoded in accordance with Standard 908 of the International Electrotechnical Commission are stored, a portion of which encoded data is altered by

introducing a modification in a sub-code Q channel of the data, such that the altered data are inconsistent with an implementation of Standard 908 used in the data readout device, but do not prevent playback of the data following recording thereof, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium.

37. A medium according to claim 36, wherein the medium comprises a compact disk.

38. A medium according to claim 36, wherein the data comprise digital audio data.

39. A medium according to claim 36, wherein the data are encoded on the medium in a multiple-session format, including both audio and data sessions, and wherein the defect is introduced in at least one of the audio and data sessions.

40. A medium according to claim 36, wherein the data are encoded on the medium in a multiple-session format, including first and second sessions, and wherein the second session contains the data from the first session in a compressed form, for use in making an authorized copy of the first session.

41. A medium according to claim 36, wherein the encoded data comprise encoded audio data, and wherein a portion of the encoded audio data is altered such that the altered data are identified as inconsistent with the implementation of Standard 908 used in the data readout device,

wherein the data recorded on the medium comprise ancillary data which are used by a processor in the application to operate upon the altered portion of the encoded audio data such that the application plays back the data in a manner substantially unaffected by the alteration of the encoded audio data, but which ancillary data are ineffective in correcting the altered portion of the encoded audio data upon copying of the data, so that the alteration causes a further substantially unrecoverable error in the unauthorized copying of the original medium.

42. A data storage medium that is resistant to unauthorized copying, on which medium data encoded in accordance with Standard 908 of the International Electrotechnical Commission are stored, a portion of which encoded data is altered to introduce a modification in the data, so that a digital output of the altered data will be inconsistent with an implementation of Standard 958 of the International Electrotechnical Commission, but the

modification will not prevent playback of the data following recording thereof, whereby an application which plays back the recorded data runs in a manner substantially unaffected by the alteration of the data, but a substantially unrecoverable error occurs in unauthorized copying of the original storage medium based on the digital output.

FIG. 1

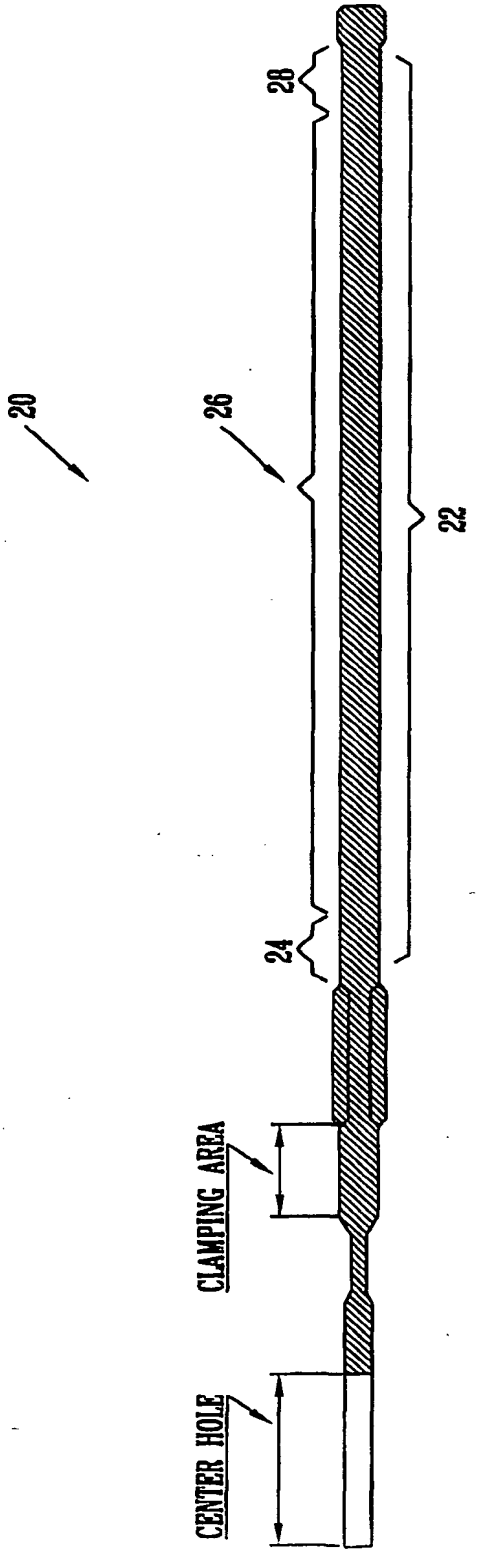


FIG. 2

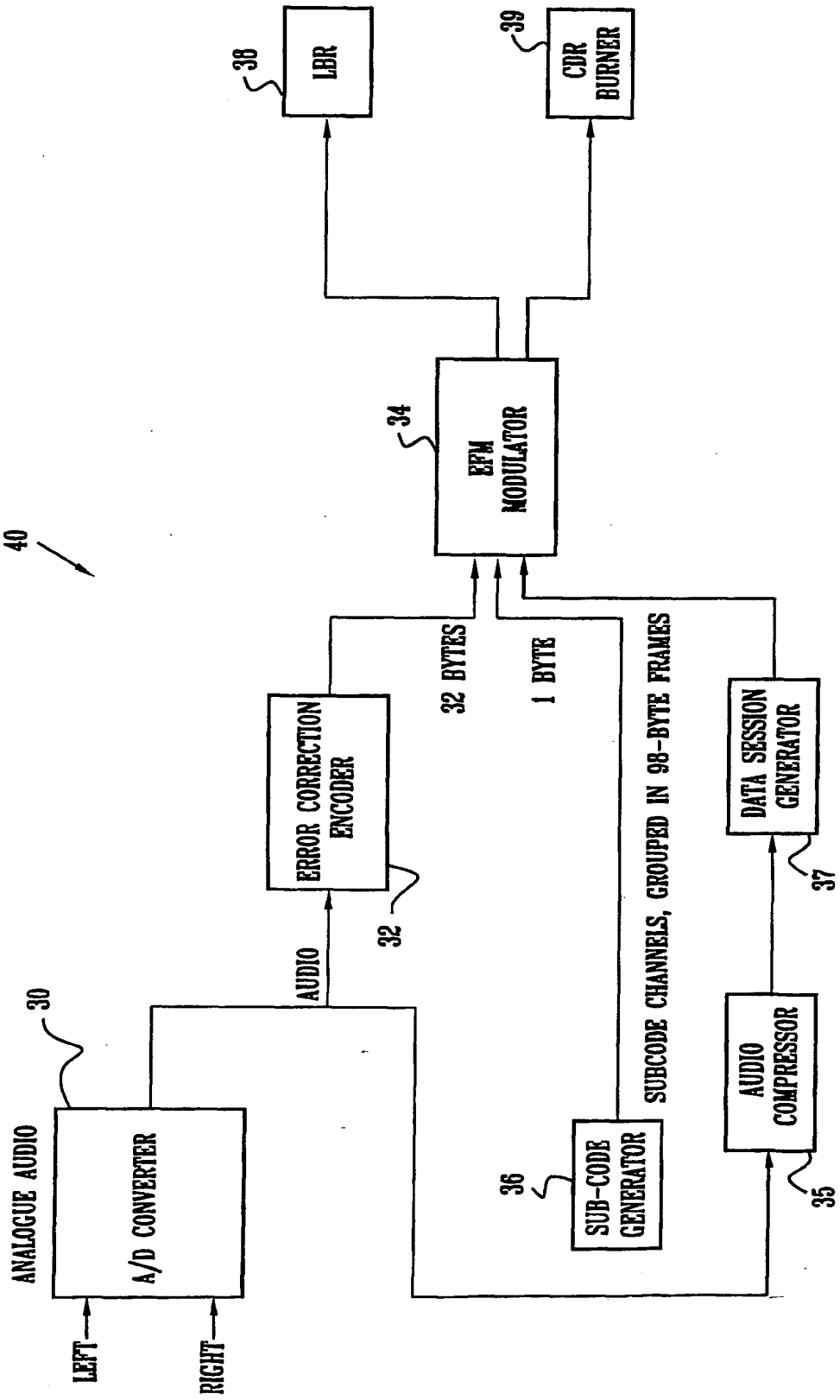

40
ANALOGUE AUDIO
A/D CONVERTER
30
LEFT
RIGHT
AUDIO
ERROR CORRECTION ENCODER
32
32 BYTES
1 BYTE
SUBCODE CHANNELS, GROUPED IN 98-BYTE FRAMES
EFM MODULATOR
34
LBR
38
CDR BURNER
39
SUB-CODE GENERATOR
36
AUDIO COMPRESSOR
35
DATA SESSION GENERATOR
37

FIG. 3

PRIOR ART

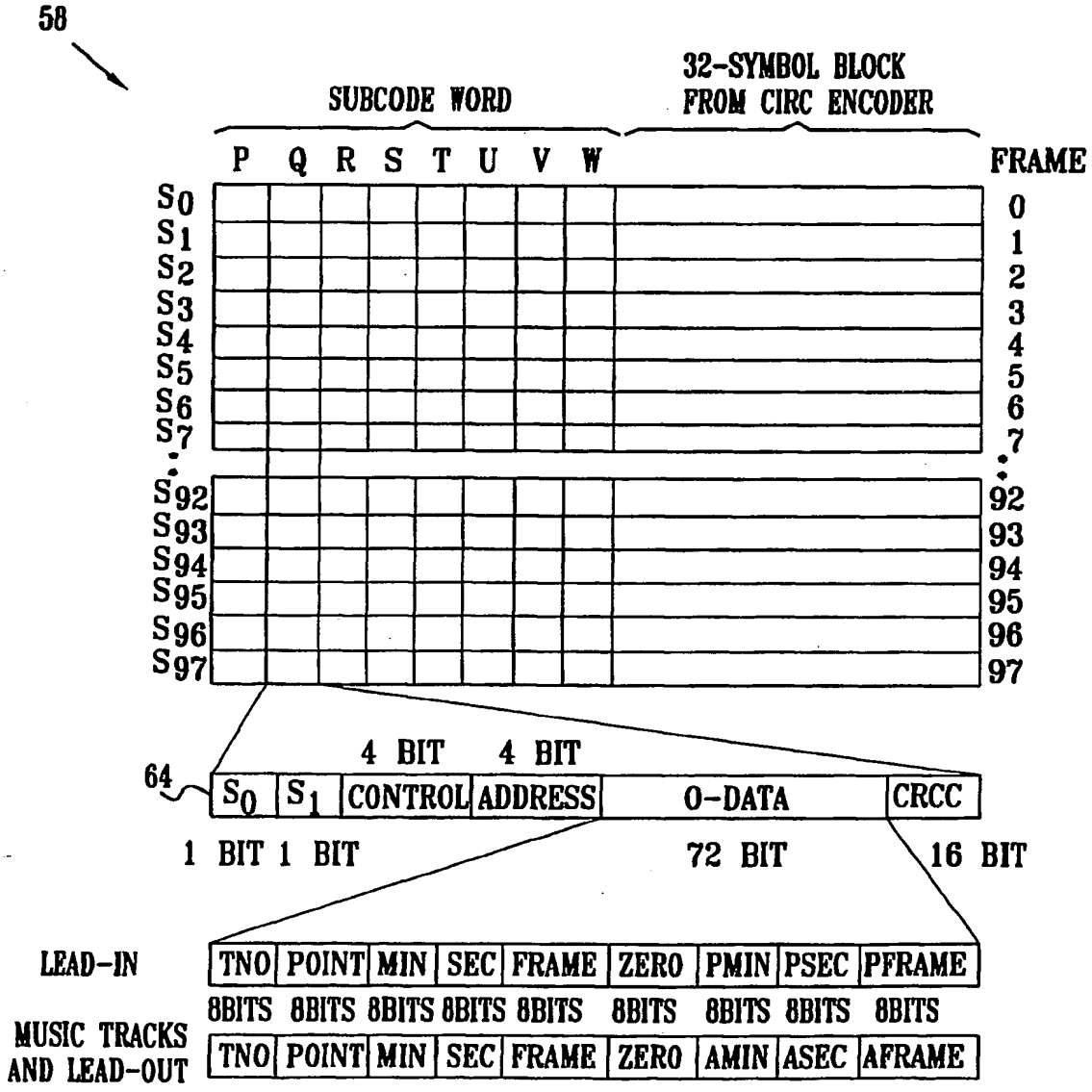
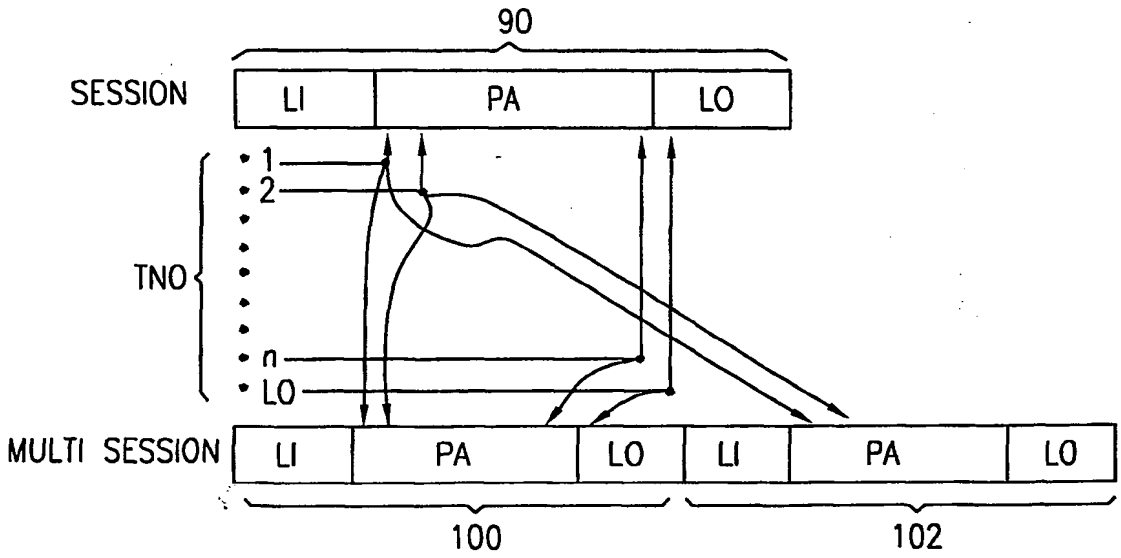


FIG. 4


90
SESSION
LI
PA
LO
1
2
TNO
n
LO
MULTI SESSION
LI
PA
LO
LI
PA
LO
100
102

Job Messages

XEROX

0180546

Document Name: 0180546

%%[Error: ioerror; OffendingCommand: xeroximage]%%

Enhanced Xerox PostScript Error Handler v1.5 Thu Apr 29 3:52 pm 1993

ERROR: ioerror
OFFENDING COMMAND: xeroximage

THE OBJECTS ON THE TOP OF THE OPERAND STACK WERE:
XeroxClosePath
--nostringval--
--nostringval--
--nostringval--
0.0

THE SOURCE LINES FOLLOWING THE ERROR ARE:
myfile closefile

showpage

pagelevel restore

EXTRA INFORMATION TO AID IN DEBUGGING THIS ERROR:

PostScript: ioerror:

An error has occurred during some attempt to access a file.

Details:

An exception other than end-of-file has occurred during execution of one of the file operators. The nature of the exception is environment dependent, but may include such events as parity or checksum errors, or broken network connections. Attempting to write to an input file or to a file that has been closed will also cause an ioerror. Occurrence of an ioerror does not cause the file to become closed unless it was already closed or the error occurs during closefile.

Job Messages

Recovery:

1. Use the bytesavailable operator on the file to the file's existence and confirm that its size is not zero.

2. Use the status operator to confirm that the file is still valid.

3. Check issues external to PostScript interpreter (such as network connection and hardware integrity).

%%[Flushing: rest of job (to end-of-file) will be ignored]%%